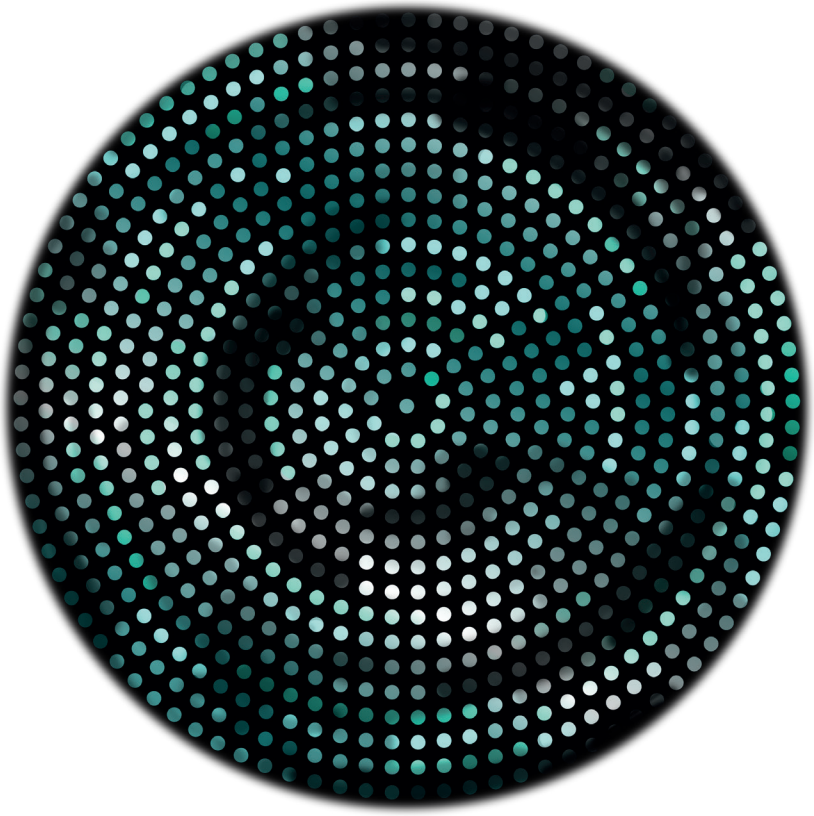
Deloitte.



Building Confidence through SOC 2 Reporting

Today, extending core and non-core functions to outsource service providers (OSPs) are playing a vital role in helping companies increase their efficiency and profitability. In fact, outsourcing of IT has evolved into a strategic business practice and OSPs have become increasingly integrated with their clients' day-to-day operations, often handling highly sensitive and critical information. This has the potential to profoundly impact their clients' internal control framework, including compliance requirements. Times are changing and the corporate Ireland scene is getting more dynamic and challenging. Business processes are getting increasingly complex and organisations are focusing on newer service delivery models as a way of managing increased technical complexity, tough competition and resource scarcity. Cloud computing, IT managed services and data centre hosting are emerging as the favoured business solutions.

However, the question is – how would organisations have assurance that information entrusted to the OSPs are secured, available, protected and processed completely and accurately? This is precisely where the SOC 2 report fits in. Most organisations that work with OSPs are familiar with SOC 1 reports, which cover internal controls over financial reporting (ICFR) and support a customer's financial audit. SOC 2 reports, on the other hand, enter a more far-reaching domain, focusing on the OSP's controls that are relevant to American Institute of Certified Public Accountants' (AICPA) Trust Service Criteria (TSC):

- Security: The system is protected against unauthorised access (both physical and logical). The security TSP serves as the basis for all SOC 2 reports and is commonly referred to as the Common Criteria.
- Availability: The system is available for operation and use as committed or agreed.
- Processing integrity: System processing is complete, accurate, timely, and authorised.
- Confidentiality: Information designated as confidential is protected as committed or agreed.
- Privacy:

Personal information is collected, used, retained, disclosed, and disposed to meet the entity's commitments and system requirements.

A SOC 2 report will be similar in structure and general approach to the traditional SOC 1 report with an option for a Type 1 or Type 2 report. A Type 1 only covers the design of controls, while a Type 2 covers design and operating effectiveness. SOC 2 can be applied for regulatory

or non-regulatory purposes to cover business areas outside of financial reporting. The report can be distributed to customers and other stakeholders to focus on system processing controls to meet their requirements. Many providers find that SOC 2 reports, typically updated every six to twelve months, often fulfil regulatory requirements while reducing many employee hours now spent completing multiple client audits, questionnaires, and surveys. More importantly, a SOC 2 report can help reinforce stakeholder confidence in an organisation's operational performance, addressing concerns before they even arise.

Bottom line benefits

- Proactively reinforce client confidence in your company's operating controls
- Reduce the amount of time required to conduct the audit and produce a final report using Deloitte-proprietary SOC 2 tools and methodologies
- Produce a comprehensive, highly usable SOC 2 report that addresses stakeholders' security, availability, confidentiality, processing integrity and privacy concerns
- Gain a comprehensive audit report certified by a highly respected global accounting firm
- Gain clear, specific insights for improving operating controls

Third-party reporting proficiency with SOC 2+

Providing assurance with regard to the AICPA TSC may be sufficient for some OSPs customers. But others may require greater detail. For this reason, the AICPA has created SOC 2+. This extensible framework allows OSPs' auditors (also known as service auditors) to incorporate various industry standards, such as the National Institute of Standards and Technology (NIST) and the International Standardisation Organisation (ISO), into one SOC 2 report. This can also provide assurance to service organisations on their General Data Protection Regulation (GDPR) obligations and Cloud Computing processes and controls.

SOC 2+ reports create substantial efficiencies for organisations. Organisations are able to spend less time and fewer resources conducting performance reviews at their OSPs. Both OSPs and customers are also less likely to be exposed to compliance violations that can result in various forms of liability, including fines.

For OSPs, the benefits are even more significant. SOC 2+ reports allow OSPs to demonstrate to their stakeholders that effective internal controls are in place. These controls pertain to the criteria covered in the TSPs of security, availability, processing integrity, confidentiality, and privacy, as well as many of the most detailed requirements covered in other regulatory and industry-specific frameworks. They offer a standardised format for meeting a broad range of regulatory and non-regulatory control requirements, eliminating the need for redundant activities and one-off responses. They're also flexible enough that they can be tailored to meet the specific needs of organisations.

Contacts

Dublin
Deloitte and Touche House
Earlsfort Terrace
Dublin 2
T: +353 1 417 2200
F: +353 1 417 2300

Cork
No.6 Lapp's Quay
Cork
T: +353 21 490 7000
F: +353 21 490 7001

Limerick
Deloitte and Touche House
Charlotte Quay
Limerick
T: +353 61 435500
F: +353 61 418310

Galway
Galway Financial Services Centre
Moneenageisha Road
Galway
T: +353 91 706000
F: +353 91 706099

Belfast
19 Bedford Street
Belfast BT2 7EJ
Northern Ireland
T: +44 (0)28 9032 2861
F: +44 (0)28 9023 4786

deloitte.ie

Deloitte.